



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/655,372	09/05/2003	Masanao Sakai	053969-0157	8586
22428 7590 08/06/2008 FOLEY AND LARDNER LLP SUITE 500 3000 K STREET NW WASHINGTON, DC 20007				
EXAMINER				
PAN, JOSEPH T				
ART UNIT		PAPER NUMBER		
2135				
MAIL DATE		DELIVERY MODE		
08/06/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/655,372

Applicant(s)

SAKAI, MASANAO

Examiner

JOSEPH PAN

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 May 2008.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-8,10-15,17-21 and 23-32 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-8,10-15,17-21 and 23-32 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 05 September 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☐ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. Applicant's response filed on May 22, 2008 has been carefully considered. Claims 1, 3-8, 10-15, 17-21, and 23-32 are pending.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1, 3-8, 10-15, 17-21 and 23-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arrow et al. (U.S. Patent No. 6,175,917 B1), hereinafter "Arrow", in view of Yamaguchi et al. (U.S. Pub. No. 2001/0042201 A1), hereinafter "Yamaguchi".

Referring to claim 1:

i. Arrow teaches:

A network comprising:

IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Intern path in the case where different two centers communicate via the Internet (see figure 1, elements 115, 125, 135, 145, 155; and column 6, line 61, through column 7, line 7, of Arrow); and

an IPsec setting server apparatus, which manages IPsec settings of said IPsec processing apparatuses (see figure 1, element 160; figure 13, elements

Art Unit: 2135

1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow);

wherein said Ipsec setting server apparatus includes means for collectively managing policies of said IPsec to be applied between first and second IPsec processing apparatuses (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15 of Arrow), and

wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatus received from said first IPsec processing apparatus (see figure 11, element 1102 'receive request' to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

ii. Yamaguchi teaches a security communication method wherein Yamaguchi discloses using IPsec to implement VPN (Virtual Private Network) (see page 1, paragraph [0008] of Yamaguchi).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yamaguchi into the method of Arrow to use IPsec.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yamaguchi into the system of Arrow to use IPsec, because Arrow teaches implementing VPN (Virtual Private Network) via IP (Internet Protocol), and Yamaguchi discloses using IPsec to implement VPN (see page 1, paragraph [0008] of Yamaguchi). Therefore, Yamaguchi's teaching would be a good match to Arrow's teaching.

Referring to claims 3-4, 10-11, 16-17, 23-24, 29:

Arrow and Yamaguchi teach the claimed subject matter: a network. They further disclose transmitting messages between IPsec setting server apparatus and IPsec processing apparatus (see column 9, lines 19-22 of Arrow).

Referring to claims 15, 28:

Arrow and Yamaguchi teach the claimed subject matter: a network. They further disclose the inquiry means (see page 4, paragraph [0045], lines 1-5 of Yamaguchi).

Referring to claims 5, 12, 25:

Arrow and Yamaguchi teach the claimed subject matter: a network. They further disclose generating SA (Security Association) parameters (see figure 13, element 1310 'define VPN parameters'; and column 15, lines 52-54 of Arrow).

Referring to claims 6, 13, 26:

Arrow and Yamaguchi teach the claimed subject matter: a network. They further disclose send a message including the policies and the SA parameters (see figure 13, elements 1310, 1314, 1316; and column 9, lines 19-22 of Arrow).

Referring to claims 7, 14, 19, 27, 31:

Arrow and Yamaguchi teach the claimed subject matter: a network. They further disclose the keys for encryption and authentication (see column 11, lines 32-34 of Arrow).

Referring to claim 8:

- i. Arrow teaches:

An IPsec setting server apparatus managing IPsec setting of IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Internet path in the case where different two centers communicate via the Internet (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow),

wherein said IPsec setting server apparatus includes means for collectively managing policies of said IPsec to be applied among said IPsec processing

Art Unit: 2135

apparatuses (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15 of Arrow), and

wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatus received from said first IPsec processing apparatus (see figure 11, element 1102 'receive request' to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

ii. Yamaguchi teaches a security communication method wherein Yamaguchi discloses using IPsec to implement VPN (Virtual Private Network) (see page 1, paragraph [0008] of Yamaguchi).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yamaguchi into the method of Arrow to use IPsec.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yamaguchi into the system of Arrow to use IPsec, because Arrow teaches implementing VPN (Virtual Private Network) via IP (Internet Protocol), and Yamaguchi discloses using IPsec to implement VPN (see page 1, paragraph [0008] of Yamaguchi). Therefore, Yamaguchi's teaching would be a good match to Arrow's teaching.

Referring to claim 15:

i. Arrow teaches:

An IPsec processing apparatus using an IPsec (Internet Protocol security protocol) on the Internet, wherein said IPsec processing apparatus includes means for, upon receiving a packet to which said IPsec should be applied,

judging whether or not to inquire a setting for said IPsec to be collectively managed in an IPsec setting server apparatus from said IPsec setting server apparatus (see column 4, lines 38-40; column 11, lines 27-30 of Arrow).

wherein said IPsec processing apparatus includes means for transmitting a request message for communication with another IPsec processing apparatus to said IPsec setting server apparatus in order to acquire a setting for said IPsec (see figure 11, element 1102 'receive request' to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54; and column 9, lines 19-22 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

ii. Yamaguchi teaches a security communication method wherein Yamaguchi discloses using IPsec to implement VPN (Virtual Private Network) (see page 1, paragraph [0008] of Yamaguchi).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yamaguchi into the method of Arrow to use IPsec.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yamaguchi into the system of Arrow to use IPsec, because Arrow teaches implementing VPN (Virtual Private Network) via IP (Internet Protocol), and Yamaguchi discloses using IPsec to implement VPN (see page 1, paragraph [0008] of Yamaguchi). Therefore, Yamaguchi's teaching would be a good match to Arrow's teaching.

Referring to claims 18, 30:

Arrow and Yamaguchi teach the claimed subject matter: an IPsec processing apparatus. They further disclose the SPD, SAD (see e.g. figure 10, elements 1010, 1005 of Yamaguchi).

Referring to claims 20, 32:

Arrow and Yamaguchi teach the claimed subject matter: an IPsec processing apparatus. They further disclose acquiring new setting information (see column 10, lines 41-51 of Arrow).

Referring to claim 21:

- i. Arrow teaches:

An IPsec setting method for a network which comprises:

IPsec processing apparatuses, which use an IPsec (Internet Protocol security protocol) for securing security on the Internet path in the case where different two centers communicate via the Internet (see figure 1, elements 115, 125, 135, 145, 155; and column 6, line 61, through column 7, line 7, of Arrow); and

an IPsec setting server apparatus, which manage IPsec settings of said IPsec processing apparatuses (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15, of Arrow),

wherein said IPsec setting server apparatus includes a step of collectively managing policies of said IPsec to be applied among said IPsec processing apparatuses (see figure 1, element 160; figure 13, elements 1314 "define access control rules", 1316 "define address translation rules"; and column 15, line 69, through column 16, line 15 of Arrow), and

wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatus received from said first IPsec processing apparatus (see figure 11, element 1102 'receive request' to configure VPN unit'; figure 13, elements 1310 'define VPN parameters', 1314 'define access control

rules', 1316 'define address translation rules'; and column 15, line 52-column 16, line 15, of Arrow, emphasis added).

Arrow discloses IP protocol and IP packets (see column 6, lines 51-54; and column 9, lines 19-22 of Arrow). However, Arrow does not specifically mention the IPsec (Internet Protocol security protocol).

ii. Yamaguchi teaches a security communication method wherein Yamaguchi discloses using IPsec to implement VPN (Virtual Private Network) (see page 1, paragraph [0008] of Yamaguchi).

iii. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Yamaguchi into the method of Arrow to use IPsec.

iv. The ordinary skilled person would have been motivated to have applied the teaching of Yamaguchi into the system of Arrow to use IPsec, because Arrow teaches implementing VPN (Virtual Private Network) via IP (Internet Protocol), and Yamaguchi discloses using IPsec to implement VPN (see page 1, paragraph [0008] of Yamaguchi). Therefore, Yamaguchi's teaching would be a good match to Arrow's teaching.

Response to Arguments

4. Applicant's arguments filed May 22, 2008 have been fully considered but they are not persuasive.

Applicant argues:

"The VPN management station configures each individual VPN unit. There is no teaching or suggestion in Arrow that the VPN units have policies that are to be applied between them." (see page 2, 3rd paragraph, Applicant's Arguments/Remarks, emphasis added)

Examiner maintains:

Arrow discloses "The particular packet processing algorithms to be used for VPN traffic may vary, so long as the lookup tables in both the sending and receiving VPN units [i.e., between two VPN units] identify the same compression, encryption and authentication rules [i.e., applying same policies between two VPN units] and are capable of implementing them for members of the same group." (see column 7, line 65 – column 8, line 3 of Arrow, emphasis added). Thus, Arrow discloses that the VPN units have policies that are to be applied between them.

Applicant argues:

"Applicants respectfully submit that there is no teaching or disclosure in Arrow that "said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatuses received from said first IPsec processing apparatus." (see page 2, last line – page 3, top 4 lines, Applicant's Arguments/Remarks, emphasis added)

Examiner maintains:

Arrow discloses "In state 1310, the system manager defines VPN parameters for authentication, encryption, and compression functions to be associated with a newly created VPN. Next, the system manager proceeds to state 1312. In state 1312, the system manager assembles groups of entities and remote clients into a VPN. States 1310 and 1312 are repeated for each VPN that the system manager desires to create.

The system manager then proceeds to state 1314. In state 1314, the system manager defines access control rules [i.e., policies] for VPN units. These access control rules specify which types of communications are allowed to pass through a VPN unit. For example, an access control rule may specify that communications between non-members of a VPN and members of a particular VPN are not allowed to pass through a particular VPN unit. Next, the system manager proceeds to state 1316.

In state 1316, the system manager specifies address translation rules [i.e., policies] for each VPN unit. These address translation rules support static translation,

dynamic translation and port translation. For example, the rules make it possible to use the same address for two different nodes that are located on different local area networks that are coupled to the public network through VPN units. The VPN units use the address translation rules to translate the same local addresses into different public network addresses. Address translation rules also facilitate mapping multiple local addresses to a single public network address. In one embodiment, this is accomplished by using the same public network address with different port identifiers for different local addresses. The system manager then proceeds to state 1320, which is an end state.” (see column 15, line 52-column 16, line 15 of Arrow, emphasis added). Therefore, Arrow discloses that the VPN management station specifying policies of IPsec to be applied between the IPsec processing apparatuses.

Arrow further discloses “The particular packet processing algorithms to be used for VPN traffic may vary, so long as the lookup tables in both the sending and receiving VPN units [i.e., between two VPN units] identify the same compression, encryption and authentication rules [i.e., applying same policies between two VPN units] and are capable of implementing them for members of the same group.” (see column 7, line 65 – column 8, line 3 of Arrow, emphasis added). Thus, Arrow discloses that the VPN units have policies that are to be applied between them.

Arrow further discloses “One function of VPN management station 160 is to manage the configuration of VPN units, such as VPN unit 115, through the issuance of configuration requests. FIG. 11 depicts an illustrative procedure for issuing a configuration request to install a new VPN unit operating system program on VPN unit 115. The procedure commences with state 1100. In state 1102 a request is received, illustratively from a user, to alter the configuration of VPN unit 115. VPN management station 160 examines the request in state 1104. If the request does not involve installation of a new operating system, the request is handled in state 1106 after which the procedure exits in state 1118.” (see column 14, lines 33-44 of Arrow, emphasis

added). Therefore, Arrow discloses the VPN management station 160 receiving or utilizing the contents of a request message for communication between the IPsec processing apparatus.

Thus, Arrow discloses "said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatuses received from said first IPsec processing apparatus."

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone

Art Unit: 2135

numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Joseph Pan

July 30, 2008

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135